(57) 摘要

一种跨网络统一用户注册信息的方法，它至少包括网络内容供应方（ICP）以及能够接入在线终端的用户登录识别器件；其中 ICP 在登录网页中加入接口模块，通过该接口模块访问用户登录识别器件，ICP 在登录网页中还设有用户登录识别器件管理驱动模块，该管理驱动模块用于监测用户登录识别器件的接入，建立连通、挂起；用户登录识别器件具有识别号，用户登录识别器件用于存放用户登录识别信息。采用本发明的方法和系统，网络服务供应商（ICP）不需要修改网页或只需要简单修改的前提下，为用户提供一种快捷、便携、安全、通用的登录方式，用户使用登录识别器件登录网站，不仅安全、灵活，而且能够随时方便地移动。

跨网络统一用户注册信息的方法及系统

技术领域

本发明涉及一种网络用户注册信息的识别、管理方法及系统，尤其是一种跨网络统一用户注册信息的方法及系统。属于计算机技术领域。

背景技术

网络日益渗透到人们的日常生活中，利用网络交换信息，传递信息，越来越成为主要的信息交互方式。实际操作中，用户登录网站时，需要输入用户名和密码，网络识别了用户，才能向用户提供特定的服务。当一个用户在多个网站注册后，这些操作就变得很烦琐。

微软推出了网络护照（ Passport）识别服务，允许用户使用一个登录名和密码在 Internet 上访问 Microsoft.com 附属站点和数量不断增加的参与 Web 站点。

Microsoft Passport 是一项单一服务，允许您使用一个登录名和密码在 Internet 上访问 Microsoft.com 附属站点和数量不断增加的参与 Web 站点。拥有一个 Passport 意味着您只需记住一个登录名和密码。该技术非常容易。因为只有一个要记住的登录名和密码，并且在登录一个参与站点后，您只需一个单击操作就可以登录到其它站点；它的速度很快。您可以将您自己的信息储存在 Passport 登录档案文件中，这样在访问参与站点时您就无需重新键入；它更安全。您的个人信息将得到功能强大的加密技术和严格的隐私保密措施的保护，并且您始终可以控制哪些站点能够访问个人信息，包括电子邮件和通信地址。并且，当您注销后，所有与您的 Passport 相关的信息都将从计算机上删除，因此在公用或共享计算机上使用个人信息也是安全的。

拥有了 .NET Passport，您就可以实现在访问每个新站点时无需注册登

录名和密码 —— 只要使用您注册 .NET Passport 时的电子邮件地址和密码登录到任意一个参与站点或服务即可。当通过在 .NET Passport 登录框中输入您的用户名和密码而登录到某个 .NET Passport 参与站点时，.NET Passport 会确认以下信息:

您键入的用户名是否被注册为 .NET Passport; 您键入的密码是否正确。 如果结论是肯定的，接下来 .NET Passport 服务就会向站点通知您的身份（您已经提供了有效的登录证书），这样您便可以访问该参与站点了。一旦您在 Internet 会话期间登录到了某个 .NET Passport 参与站点，那么通过单击每个参与站点上的“.NET Passport 登录”按钮就可以登录到其他站点。

用户使用步骤是这样的:

1、注册 .NET Passport 用户名、密码（用户名是 Email 地址）

2、登录到任意一个参与站点或服务

3、通过 .NET Passport 登录框中输入用户名和密码

4、如果该用户名被注册为 .NET Passport，且键入的密码正确，就可以访问该参与站点了（登录成功）

5、在 Internet 会话期间，登录其它参与站点或服务，不再需要重新输入密码。

虽然，拥有一个 Passport 意味着用户只需记住一个登录名和密码。但由于现有的网站数据格式不尽相同，要做到统一，修改量大，限制了参与 Passport 的 Web 站点。Windows 提供了记住用户名和密码的功能，但由于只能存在本机，缺少安全性和便携性，只能适用于一部分私人计算机。

发明内容

本发明的主要目的是提供一种跨网络统一用户注册信息的方法及系统，在网络内容供应商（ICP）不需要修改网页或只需要简单修改的前提下，

为用户提供一种快捷、便携、安全、通用的登录方式。

本发明的又一目的在于提供一种跨网络统一用户注册信息的方法及系统，使用灵活、安全，能够随时移动、方便地登录。

本发明的目的是这样实现的：

一种跨网络统一用户注册信息的方法，它至少包括网络内容供应方（ICP）以及能够接入在线终端的用户登录识别器件；其中 ICP 在登录网页中加入接口模块，通过该接口模块访问用户登录识别器件，ICP 在登录网页中还设有用户登录识别器件管理驱动模块，该管理驱动模块用于监测用户登录识别器件的接入，建立连通、挂起；用户登录识别器件具有识别号，用户登录识别器件用于存放用户登录识别信息。

ICP 的鉴权包括通过接口模块获取鉴权文件，传递给管理驱动模块，管理驱动模块对鉴权文件进行解密后，访问用户登录识别器件。

管理驱动模块还可将用户登录识别器件内存储的数据进行导入和/或导出，以便进行数据备份。管理驱动模块还包括在 ICP 通过接口模块访问用户登录识别器件，并验证识别信息完成后，自动进行登录。

另外，本发明也可以使用在线方式完成 ICP 与登录验证服务方的鉴权。ICP 连接一登录验证服务方，登录验证服务方发送访问用户登录识别器件的代码给网络内容供应方（ICP），ICP 依据该代码在登录网页中加入登录识别信息，接口模块将 ICP 信息传递给登录验证服务方进行验证，验证合格，允许 ICP 访问用户登录识别器件。登录验证服务方维护一个鉴权文件库，用于实现管理鉴权文件。

由登录验证服务方和/或 ICP 网站提供接口模块和管理驱动模块，检测是否已下载接口模块和管理驱动模块，如果有，则进行激活；如果没有，先下载接口模块和管理驱动模块，再进行激活。用户登录识别器件处于激活状态时，ICP 首先与登录验证服务方完成鉴权，才能访问用户登录识别

器件。

具体地，访问用户登录识别器件包括存放或读取用户登录识别器件内的登录注册信息。登录验证服务方发送鉴权文件给 ICP，ICP 根据该文件访问用户登录识别器件。鉴权文件内包括有 ICP 识别信息和/或用户登录识别器件特定区域引导信息和/或数据处理引导信息。

另外，用户登录识别器件内存储 ICP 识别信息注册表，用于引导不同的 ICP 对该器件中访问时，仅访问对应的区域或内容。管理驱动模块还可将用户登录识别器件内存储的数据进行导入和/或导出，以便进行数据备份，还包括在 ICP 通过接口模块访问用户登录识别器件，并验证识别信息完成后，自动进行登录。

进一步地，ICP 通过接口模块读取用户登录识别器件中的信息，如果得到登录识别信息，接口模块将登录识别信息返回给 ICP 网页，根据用户的设置决定是否自动提交并登录；若没有得到登录识别信息，接口模块通知网页未读取登录识别信息，将产生的登录识别信息存放到用户登录识别器件中。

存储登录识别信息包括用户初次登录 ICP 网站，或用户选择重新手动输入登录信息，或初次使用用户登录识别器件，ICP 通过接口模块将登录识别信息存储到用户登录识别器件中。

ICP 网页设有注册信息窗口，调用接口模块参数，同时保存同一网页多套注册信息，或保存最近的一套注册信息。

例如，ICP 在网页上设有一注册信息窗口，ICP 通过接口模块访问用户登录识别器件，比较 ICP 网页提供的登录识别信息，将新登录识别信息数据存储到用户登录识别器件中，覆盖原有登录识别信息，将相关信息传递给 ICP 网页，网页获取该信息后，显示该信息。

再有，ICP 在网页上设有多个注册信息的窗口连接，ICP 读取用户登录识别器件内存储用户登录识别信息，比较 ICP 网页提供的登录识别信息，

不相同，则将该登录识别信息存储到用户登录识别器件中，相同时，直接读取，将相关信息传递给 ICP 网页，网页获取该信息后，显示该信息。

其中，用户登录识别信息包括 ICP 识别信息或表单信息或用户识别信息或其组合。

一种实现上述任一方法的系统，它包括计算机、互联网网络、ICP 以及用户登录识别器件，其中计算机能够登录到互联网网络上，与不同的 ICP 通信；用户登录识别器件为能够从外部连接到计算机上、至少具有识别号码以及加密存储空间的器件，通过操控计算机进行用户登录识别器件的信息传递。

计算机到用户登录识别器件的信息传递经过加密或解密的处理。加密为通过用户的 PIN 密码保护加密区或采用 RSA 512PKI 密钥管理方式加密。用户登录识别器件还设有 ICP 存放自有信息存储区。

具体地，用户登录识别器件可为带有标准数据接口外接便携式可移动存储部件或其读卡器件或身份识别器件。例如 U 盘或 CF 卡或 MMC 卡或 SD 卡或 SMC 卡或 IBM Micro Drive 卡或闪存模块或 IC 卡，或其相应的读卡器本身内部。

另外，用户登录识别器件为计算机外设，如键盘或鼠标或手写板或音箱，便携式 PDA 或音乐播放器或电子词典。

进一步地，本发明系统的 ICP 连接一登录验证服务方，登录验证服务方发送访问用户登录识别器件的代码给网络内容供应方（ICP），ICP 依据该代码在登录网页中加入登录识别信息，接口模块将 ICP 信息传递给登录验证服务方进行验证，验证合格，允许 ICP 访问用户登录识别器件。其中登录验证服务方为服务器。

根据上述技术方案分析可知，本发明具有如下优点：

1、统一的注册信息，简化了用户登录网络的繁琐操作。

2、便携式的硬件，使用户可以随身携带，随时随地使用。

3、硬件和数据加密的双重保护，保证了用户个人信息的安全性。

4、管理驱动模块，提供了实用的功能管理，使用户的使用直观、简捷。

5、ICP 不需修改其现有的数据格式。

6、ICP 得到的是一个灵活的接口，除了用于用户登录，还可以扩展出自定义的丰富应用。

附图说明

图 1 为本发明网络系统构成示意图；

图 2 为本发明用户访问 ICP 下载管理驱动模块流程图；

图 3 为本发明 ICP 访问用户登录识别器件的流程图；

图 4 为本发明用户通过登录识别器件登录 ICP 的流程图。

具体实施方式

下面结合附图和具体实施方式对本发明做进一步地详细说明。

如图 1 所示，本发它包括计算机、互联网网络、ICP 以及用户登录识别器件。计算机能够登录到互联网网络上，与不同的 ICP 通信；用户登录识别器件为能够从外部连接到计算机上、至少具有识别号码以及加密存储空间的器件，通过操控计算机进行用户登录识别器件的信息传递。其中 ICP 在登录网页中加入接口模块，通过该接口模块访问用户登录识别器件，ICP 在登录网页中还设有用户登录识别器件管理驱动模块，该管理驱动模块用于监测用户登录识别器件的接入，建立连通、挂起；用户登录识别器件具有识别号，用户登录识别器件用于存放用户登录识别信息。

用户登录识别器件具体地可为带有标准数据接口外接便携式可移动存储部件或其读卡器件或身份识别器件。例如 U 盘或 CF 卡或 MMC 卡或 SD 卡或 SMC 卡或 IBM Micro Drive 卡或闪存模块或 IC 卡，或其相应的读卡器本

身内部。

另外，也为计算机外设，如键盘或鼠标或手写板或音箱，便携式 PDA 或音乐播放器或电子词典。

其中用户登录识别器件可具有唯一识别号，也可具有多个识别号，通过分区控制供不同的人使用。

采用本发明的方法和系统如同提供了通行的、唯一识别的网络身份证，任何用户可采用登录识别器件自动登录所有经过授权的 ICP 或具有访问登录识别器件权限的 ICP。

本发明登录验证服务方如同 CA，它与 ICP、用户登录识别器件之间可在线进行授权、鉴权；ICP 与用户登录识别器件之间也可离线—不通过登录验证服务方，根据用户登录识别器件内的信息以及 ICP 的权限自行完成鉴权。

其中，结合图 2、3 说明本发明 ICP、用户登录识别器件之间进行鉴权，完成登录的过程。它至少包括网络内容供应方（ICP）以及能够接入在线终端的用户登录识别器件；其中 ICP 在登录网页中加入接口模块，通过该接口模块访问用户登录识别器件，ICP 在登录网页中还设有用户登录识别器件管理驱动模块，该管理驱动模块用于监测用户登录识别器件的接入，建立连通、挂起；用户登录识别器件具有唯一识别号，用户登录识别器件用于存放用户登录识别信息。管理驱动模块还可将用户登录识别器件内存储的数据进行导入和/或导出，以便进行数据备份。管理驱动模块还包括在 ICP 通过接口模块访问用户登录识别器件，并验证识别信息完成后，自动进行登录。

步骤如下：

1、插入用户登录识别器件，下载管理驱动模块；

2、输入 PIN 密码，激活用户登录识别器件，进入需要登录信息的网页；用户登录识别器件内存储 ICP 鉴权访问信息，用以验证被来访问的 ICP 是

否具有访问资格。鉴权文件内包括有 ICP 识别信息和/或用户登录识别器件特定区域引导信息和/或数据处理引导信息和/或时间信息。用户登录识别器件内存储 ICP 识别信息注册表，用于引导不同的 ICP 对该器件中访问时，仅访问对应的区域或内容。不同的 ICP 在用户登录识别器件中各自相应位置存储和读取登录识别信息；

3、ICP 访问用户登录识别器件，进行鉴权；验证通过的，可以访问；不通过的，不能够访问。其中访问包括核对用户登录识别器件内的用户身份识别信息，或在用户登录识别器件内生成用户身份识别信息。具体地，ICP 的鉴权包括通过接口模块获取鉴权文件，传递给管理驱动模块，管理驱动模块对鉴权文件进行解密后，访问用户登录识别器件；

4、ICP 读取用户登录识别器件中的信息，如果得到登录识别信息，接口模块将登录识别信息返回给 ICP 网页，根据用户的设置决定是否提交登录或自动提交并登录；若没有得到登录识别信息，接口模块通知网页未读取登录识别信息，将产生的登录识别信息存放到用户登录识别器件中。存储登录识别信息包括用户初次登录 ICP 网站，或用户选择重新手动输入登录信息，或初次使用用户登录识别器件，ICP 通过接口模块将登录识别信息存储到用户登录识别器件中。

如果 ICP 网页设有注册信息窗口，调用接口模块参数，在用户登录识别器件中同时保存同一网页多套注册信息，或保存最近的一套注册信息，还可显示在 ICP 网页上。具体地：

ICP 在网页上设有一注册信息窗口，ICP 通过接口模块访问用户登录识别器件，比较 ICP 网页提供的登录识别信息，将新登录识别信息数据存储到用户登录识别器件中，覆盖原有登录识别信息，将相关信息传递给 ICP 网页，网页获取该信息后，显示该信息。

ICP 在网页上设有多个注册信息的窗口连接，ICP 读取用户登录识别器件内存储用户登录识别信息，比较 ICP 网页提供的登录识别信息，不相同，

则将该登录识别信息存储到用户登录识别器件中，相同时，直接读取，将相关信息传递给 ICP 网页，网页获取该信息后，显示该信息。

本发明的另一实施例为登录验证服务方、ICP、用户登录识别器件之间可在线授权、鉴权完成登录的方法及系统。步骤如下：

本发明由登录验证服务方授权 ICP 加入使用管理驱动模块。获得授权的 ICP 通过接口模块（例如，OCX）的接口存储和读取用户的登录信息。在这种方案下，在 ICP 对网页仅需要进行简单的修改。用户使用一个内含 1M BYTE 以上加密存储空间的用户登录识别器件，用以存储用户的登录信息。加密存储空间的数据可以通过 API 进行访问。用户可以用 PIN 密码激活管理驱动模块的用户登录识别器件。

登录验证服务方提供一个加密的鉴权文件给各个 ICP，用以授权和授权验证。由于不同的 ICP 的鉴权文件不同，因此每一个 ICP 只能访问自己的数据，无权访问其它 ICP 的数据；提供一个 OCX，ICP 在自己的网页中加入该 OCX，通过调用 OCX 的接口去用户登录识别器件中的相应位置存储和读取相关信息。该 OCX 还负责将 ICP 的鉴权文件传到登录验证服务方的服务器作验证。

登录验证服务方的服务器端用以验证各个 ICP 的身份。

管理驱动模块的用户登录识别器件基于 USB 接口、内含 1M 以上加密存储空间（可以通过 API 进行访问），加密可以通过两种方法实现。简单加密：仅通过用户的 PIN 密码来保护加密区。若密码正确，加密存储空间的数据就可以被访问；PKI 加密：RSA 512 PKI 密钥管理,数据流加密,多密钥权限管理

其中管理驱动模块的实现为：

安装管理驱动模块软件：以后，用户桌面上会多一个相应的 Tray Icon；用户可以激活或关闭管理驱动模块。用户激活管理驱动模块时需输

入密码；监测用户登录识别器件端口，当用户插入管理驱动模块用户登录识别器件时，要求用户输入密码激活管理驱动模块用户登录识别器件。若用户取消或输入密码不正确，管理驱动模块用户登录识别器件不被激活（关闭状态）。当用户取出管理驱动模块用户登录识别器件时，关闭管理驱动模块用户登录识别器件；供用户修改 PIN 密码的功能；提供用户设置管理驱动模块的提交模式、内容填充、记录模式；在简单加密时，还会提供用户导入和导出管理驱动模块用户登录识别器件中存储的信息的功能。

加密的鉴权文件由登录验证服务方提供给 ICP，其中包含授权信息。

接口模块：提供 ICP 读写管理驱动模块用户登录识别器件的接口；传递 ICP 的鉴权文件给登录验证服务方服务器端进行验证；通过 API 读写管理驱动模块用户登录识别器件

服务器端验证 ICP 的身份，并将结果告知 OCX。

本发明的步骤：

1、登录验证服务方分发鉴权文件给 ICP 做 ICP 身份认证；

2、登录验证服务方提供标准的通过 OCX 接口访问管理驱动模块用户登录识别器件的代码样本给 ICP，ICP 参照代码样本在网页中加入所需数据的存储和读取代码，并在网页中加入 OCX 的连接；

3、用户登录识别器件带有初始的 PIN 密码；

4、用户访问 ICP 的网站，将自动下载用户的管理驱动模块软件和 OCX（也可去登录验证服务方的网站下载）。提示用户是否安装管理驱动模块软件，如确定则安装。安装完毕，用户桌面上会多一个相应的 Tray Icon；

5、用户接上管理驱动模块用户登录识别器件，可以通过管理驱动模块软件激活管理驱动模块、关闭管理驱动模块、修改 PIN 密码、导入和导出管理驱动模块用户登录识别器件中存储的信息；

6、用户访问 ICP 的网站，ICP 通过 OCX 的接口读取用户的管理驱动模块用户登录识别器件。若在激活管理驱动模块的状态下，OCX 会将 ICP 的鉴

权文件传递给登录验证服务方的服务器端作确认，如是授权的 ICP，服务器端将通知 OCX 可以访问用户登录识别器件；

7、若读取到需要的信息，OCX 返回内容给 ICP 网页代码，并根据用户的设置来决定是否自动提交并登录。若未读取到需要的信息（用户未登录过），OCX 告知 ICP 网页代码未读取到需要的信息；

8、用户初次使用一套登录信息登录或是用户选择重登录（用户手动输入登录信息）ICP 的网站，ICP 通过 OCX 的接口存储数据到用户的管理驱动模块用户登录识别器件。若在激活管理驱动模块的状态下，OCX 会将 ICP 的鉴权文件传递给登录验证服务方的服务器端作确认，如是授权的 ICP，服务器端将通知 OCX 可以访问用户登录识别器件。OCX 将数据存储到管理驱动模块用户登录识别器件。

若一个用户在同一个注册网页有多套注册信息，是同时保存，或是保存最近使用的一套，取决于 ICP 在网页中加入的调用 OCX 的接口参数。

具体实施例：

用户：小王，ICP：sina、263 小王的个人资料：在 sina 有两个会员用户名。用户名 1：丁丁 密码：ding2002；用户名 2：joy 密码：991817 在 263 有两个信箱。信箱 1：xiaowang@263.net 密码：991817；信箱 2：xiaowang111@263.net密码：991817。管理驱动模块的用户登录识别器件：初始密码：12345678。

登录验证服务方分发鉴权文件给 sina ，分发鉴权文件给 263（两个鉴权文件不同）。登录验证服务方同时提供标准的通过 OCX 接口访问管理驱动模块用户登录识别器件的代码样本给 sina 、263。

sina 在自己的网站中加入 OCX 和用户的管理驱动模块软件的自动下载（连接到登录验证服务方网站）。sina 在自己的网站的会员登录网页加入相关代码，用户打开该网页时，sina 会通过 OCX 去读去管理驱动模块用户登录识别器件中的信息。用户手动登录时，sina 通过 OCX 将信息（包括表

单编号、用户信息）存储到管理驱动模块用户登录识别器件中，sina 设定如果已存在相同表单编号的信息，该网站没有多注册信息连接窗口，因此用新的信息覆盖旧的信息。

263 在自己的网站中加入 OCX 和用户的管理驱动模块软件的自动下载（连接到登录验证服务方网站）。263 在自己的网站的会员登录网页加入相关代码，用户打开该网页时，263 会通过 OCX 去读取管理驱动模块用户登录识别器件中的信息，用户手动登录时，263 通过 OCX 将信息（包括表单编号、用户信息）存储到管理驱动模块用户登录识别器件中。263 具有多注册信息连接窗口，因此 263 设定如果已存在相同表单编号的信息，新的信息另存为一条。

小王访问 www.sina.com.cn，自动下载管理驱动模块软件和 OCX。下载完毕后，显示对话框“是否安装管理驱动模块软件”，小王选择确定，安装管理驱动模块软件。安装完毕，桌面上多了一个名为“管理驱动模块”的 Tray Icon。小王插入管理驱动模块用户登录识别器件，管理驱动模块软件提示“输入密码：”，小王输入“12345678”，选择确定，管理驱动模块被激活。Tray Icon 显示为激活状态。小王点击“管理驱动模块”的 Tray Icon，选择“修改密码”， 输入密码：12345678；输入新密码：wang1817；确认新密码：wang1817。确认后，密码修改为 wang1817，Tray Icon 仍显示为激活状态。

小王在 sina 主页选择用户登录。sina 在会员登录网页加入的相关代码通过 OCX 的接口（传入表单编号等参数），试图读取小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 sina 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，没有发现需要的信息，OCX 告知 sina 网页代码未读取到需要的信息。小王输入登录信息：用户名：丁丁密码：ding2002，登录。sina

在会员登录网页加入的相关代码通过 OCX 的接口（传入表单编号、用户信息等参数），试图将数据存储到小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 sina 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，没有发现相同表单编号的信息，OCX 将数据存储到小王的管理驱动模块用户登录识别器件。小王关闭 sina，重进入 sina 主页，检测到已下载了管理驱动模块软件和 OCX，不再需要自动下载管理驱动模块软件和 OCX。小王选择用户登录。sina 在会员登录网页加入的相关代码通过 OCX 的接口（传入表单编号等参数），试图读取小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 sina 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，发现需要的信息，OCX 将信息传给 sina 网页代码。sina 网页代码获取信息后，以用户名：丁丁 密 码：ding2002 自动登录。小王选择重登录，输入登录信息：用户名：joy 密码：991817，登录。sina 在会员登录网页加入的相关代码通过 OCX 的接口（传入表单编号、用户信息等参数），试图将数据存储到小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 sina 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，发现相同表单编号的信息，OCX 将新的数据存储到小王的管理驱动模块用户登录识别器件，覆盖旧的数据。小王点击“管理驱动模块”的 Tray Icon，选择“关闭管理驱动模块”，Tray Icon 显示为关闭状态。

小王访问 www.263.net。检测到已下载了管理驱动模块软件和 OCX，不再需要自动下载管理驱动模块软件和 OCX。263 在主页加入的邮件登录相关

代码通过 OCX 的接口（传入表单编号等参数），试图读取小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，发现处于关闭状态。OCX 告知 263 网页代码未读取到需要的信息。小王点击“管理驱动模块”的 Tray Icon，选择“激活管理驱动模块”，Tray Icon 显示为激活状态。小王输入邮件登录信息：用户名：xiaowang@263.net 密码：991817。登录。263 在主页加入的邮件登录相关代码，通过 OCX 的接口（传入表单编号、用户信息等参数），试图将数据存储到小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，发现处于激活状态。OCX 获取 263 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，没有发现相同表单编号的信息，OCX 将数据存储到小王的管理驱动模块用户登录识别器件。小王选择重登录，输入登录信息：用户名：xiaowang111@263.net密码：991817，登录。263 在主页加入的邮件登录相关代码通过 OCX 的接口（传入表单编号、用户信息等参数），试图将数据存储到小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 263 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，发现相同表单编号的信息，OCX 将新的数据存储到小王的管理驱动模块用户登录识别器件，不改变旧的数据。小王关闭 263，重进入 263 主页，检测到已下载了管理驱动模块软件和 OCX，不再需要自动下载管理驱动模块软件和 OCX。小王选择用户登录。263 在主页加入的邮件登录相关代码通过 OCX 的接口（传入表单编号等参数），试图读取小王的管理驱动模块用户登录识别器件。OCX 访问管理驱动模块用户登录识别器件，确认处于激活状态。OCX 获取 263 的鉴权文件，传递给管理驱动模块。管理驱动模块根据鉴权文件和表单编号去小王的管理驱动模块用户登录识别器件查找相关信息，发现 2 处需要的信息，OCX

将信息传给 263 网页代码。263 网页代码获取信息后，在用户名处的下拉框中显示两个用户名：xiaowang@263.net 、xiaowang111@263.net。小王点击 xiaowang@263.net，以用户名：xiaowang@263.net密码：991817 自动登录。小王取出管理驱动模块用户登录识别器件，管理驱动模块软件关闭管理驱动模块。Tray Icon 显示为关闭状态。

鉴权文件是一个加密文件。鉴权文件可以包含有效时间、有效数据段等主要信息。其中有效时间限定了该鉴权文件的有效期，过了有效期的鉴权文件将失效，需由登录验证服务方重新分发鉴权文件给 ICP；有效数据段限定了 ICP 在用户登录识别器件上可以访问的有效数据段。鉴权文件被 OCX 传递到管理驱动模块，管理驱动模块可对鉴权文件进行解密。这一过程同样可以有以下方式实现：

登录验证服务方分发鉴权文件给 ICP，当 ICP 试图访问用户登录识别器件时，OCX 将该鉴权文件传给登录验证服务方作验证，登录验证服务方再将验证结果传回。此种情况下分发给 ICP 的鉴权文件可以只包含简单的索引和认证信息，而登录验证服务方需要维护一个鉴权文件库，提供更多的更新信息。

最后所应说明的是，以上实施例仅用以说明本发明而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明进行修改或者等同替换，而不脱离本发明的精神和范围，其均应涵盖在本发明的权利要求范围当中。

权 利 要 求 书

1、一种跨网络统一用户注册信息的方法，其特征在于：它至少包括网络内容供应方（ICP）以及能够接入在线终端的用户登录识别器件；其中 ICP 在登录网页中加入接口模块，通过该接口模块访问用户登录识别器件，ICP 在登录网页中还设有用户登录识别器件管理驱动模块，该管理驱动模块用于监测用户登录识别器件的接入，建立连通、挂起；用户登录识别器件具有识别号，用户登录识别器件用于存放用户登录识别信息。

2、根据权利要求 1 所述的方法，其特征在于：用户登录识别器件内存储 ICP 鉴权访问信息，用以验证被来访问的 ICP 是否具有访问资格；验证通过的，可以访问；不通过的，不能够访问。

3、根据权利要求 1 或 2 或 3 所述的方法，其特征在于：用户登录识别器件处于激活状态时，ICP 完成鉴权，才能访问用户登录识别器件。

4、根据权利要求 1 所述的方法，其特征在于：ICP 的鉴权包括通过接口模块获取鉴权文件，传递给管理驱动模块，管理驱动模块对鉴权文件进行解密后，访问用户登录识别器件。

5、根据权利要求 4 所述的方法，其特征在于：鉴权文件内包括有 ICP 识别信息和/或用户登录识别器件特定区域引导信息和/或数据处理引导信息和/或时间信息。

6、根据权利要求 1 所述的方法，其特征在于：用户登录识别器件内存储 ICP 识别信息注册表，用于引导不同的 ICP 对该器件中访问时，仅访问对应的区域或内容。

7、根据权利要求 1 所述的方法，其特征在于：不同的 ICP 在用户登录识别器件中各自相应位置存储和读取登录识别信息。

8、根据权利要求 1 所述的方法，其特征在于：管理驱动模块还可将用户登录识别器件内存储的数据进行导入和/或导出，以便进行数据备份。

9、根据权利要求 1 或 8 所述的方法，其特征在于：管理驱动模块还包

括在 ICP 通过接口模块访问用户登录识别器件，并验证识别信息完成后，自动进行登录。

10、根据权利要求 1 或 4 所述的方法，其特征在于：ICP 访问用户登录识别器件包括核对用户登录识别器件内的用户身份识别信息，或在用户登录识别器件内生成用户身份识别信息。

11、根据权利要求 10 所述的方法，其特征在于：ICP 读取用户登录识别器件中的信息，如果得到登录识别信息，接口模块将登录识别信息返回给 ICP 网页，根据用户的设置决定是否提交登录或自动提交并登录；若没有得到登录识别信息，接口模块通知网页未读取登录识别信息，将产生的登录识别信息存放到用户登录识别器件中。

12、根据权利要求 10 或 11 所述的方法，其特征在于：存储登录识别信息包括用户初次登录 ICP 网站，或用户选择重新手动输入登录信息，或初次使用用户登录识别器件，ICP 通过接口模块将登录识别信息存储到用户登录识别器件中。

13、根据权利要求 10 所述的方法，其特征在于：ICP 网页设有注册信息窗口，调用接口模块参数，在用户登录识别器件中同时保存同一网页多套注册信息，或保存最近的一套注册信息,还可显示在 ICP 网页上。

14、根据权利要求 13 所述的方法，其特征在于：ICP 在网页上设有一注册信息窗口，ICP 通过接口模块访问用户登录识别器件，比较 ICP 网页提供的登录识别信息，将新登录识别信息数据存储到用户登录识别器件中，覆盖原有登录识别信息，将相关信息传递给 ICP 网页，网页获取该信息后，显示该信息。

15、根据权利要求 13 所述的方法，其特征在于：ICP 在网页上设有多个注册信息的窗口连接，ICP 读取用户登录识别器件内存储用户登录识别信息，比较 ICP 网页提供的登录识别信息，不相同，则将该登录识别信息存储到用户登录识别器件中，相同时，直接读取，将相关信息传递给 ICP

网页，网页获取该信息后，显示该信息。

16、根据权利要求 1 所述的方法，其特征在于：它还可包括一登录验证服务方，用于实现 ICP 在先鉴权，获得访问用户登录识别器件引导信息。

17、根据权利要求 16 所述的方法，其特征在于： ICP 连接一登录验证服务方，登录验证服务方发送访问用户登录识别器件的代码给网络内容供应方（ICP），ICP 依据该代码在登录网页中加入登录识别信息，接口模块将 ICP 信息传递给登录验证服务方进行验证，验证合格，允许 ICP 访问用户登录识别器件。

18、根据权利要求 17 所述的方法，其特征在于：用户使用密码激活用户登录识别器件后，ICP 通过接口模块至登录验证服务方进行鉴权，鉴权通过，ICP 通过接口模块对用户登录识别器件进行操控。

19、根据权利要求 18 所述的方法，其特征在于：用户使用的激活密码由登录验证服务方提供或预先定制在器件内。

20、根据权利要求 17 或 18 所述的方法，其特征在于：登录验证服务方发送给各个 ICP 的密码文件不同。

21、根据权利要求 16 所述的方法，其特征在于：登录验证服务方维护一个鉴权文件库，用于实现管理鉴权文件。

22、根据权利要求 16 或 21 所述的方法，其特征在于：登录验证服务方为服务器。

23、根据任一权利要求所述的方法，其特征在于：用户登录识别信息包括 ICP 识别信息或表单信息或用户识别信息或其组合。

24、一种实现上述任一权利要求所述方法的系统，其特征在于：它包括计算机、互联网网络、ICP 以及用户登录识别器件，其中计算机能够登录到互联网网络上，与不同的 ICP 通信；用户登录识别器件为能够从外部连接到计算机上、至少具有识别号码以及加密存储空间的器件，通过操控计算机进行用户登录识别器件的信息传递。

25、根据权利要求 24 所述的系统，其特征在于：ICP 连接一登录验证服务方，登录验证服务方发送访问用户登录识别器件的代码给网络内容供应方（ICP），ICP 依据该代码在登录网页中加入登录识别信息，接口模块将 ICP 信息传递给登录验证服务方进行验证，验证合格，允许 ICP 访问用户登录识别器件。

26、根据权利要求 25 所述的系统，其特征在于：登录验证服务方为服务器。

27、根据权利要求 24 所述的系统，其特征在于：计算机到用户登录识别器件的信息传递经过加密或解密的处理。

28、根据权利要求 25 所述的系统，其特征在于：加密为通过用户的 PIN 密码保护加密区或采用 RSA 512PKI 密钥管理方式加密。

29、根据权利要求 24 所述的系统，其特征在于：用户登录识别器件还设有 ICP 存放自有信息存储区。

30、根据权利要求 24 或 27 或 28 或 29 所述的系统，其特征在于：用户登录识别器件可为带有标准数据接口外接便携式可移动存储部件或其读卡器件或身份识别器件。

31、根据权利要求 30 所述的系统，其特征在于：用户登录识别器件为 U 盘或 CF 卡或 MMC 卡或 SD 卡或 SMC 卡或 IBM Micro Drive 卡或闪存模块或 IC 卡。

32、根据权利要求 30 所述的系统，其特征在于：移动存储读卡器为 CF 卡处理器或 MMC 卡处理器或 SD 卡处理器或 SMC 卡处理器或 IBM Micro Drive 卡处理器或 IC 卡读卡器。

33、根据权利要求 24 或 27 或 28 或 29 所述的系统，其特征在于：用户登录识别器件为计算机外设，如键盘或鼠标或手写板或音箱。

34、根据权利要求 24 或 27 或 28 或 29 所述的系统，其特征在于：用户登录识别器件为便携式 PDA 或音乐播放器或电子词典。

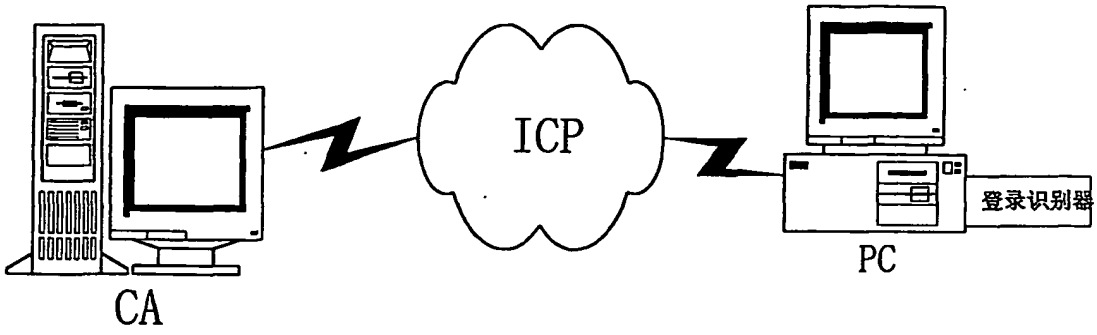

图 1

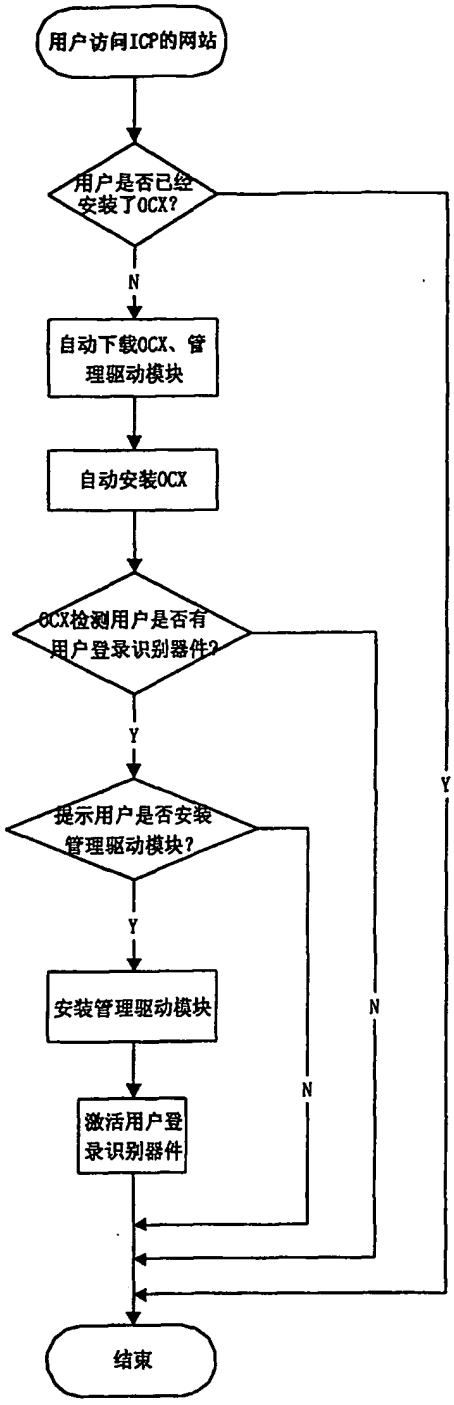
用户访问ICP的网站
用户是否已经安装了OCX?
N
Y
自动下载OCX、管理驱动模块
自动安装OCX
OCX检测用户是否有用户登录识别器件?
Y
N
提示用户是否安装管理驱动模块?
Y
N
安装管理驱动模块
激活用户登录识别器件
结束

图 2

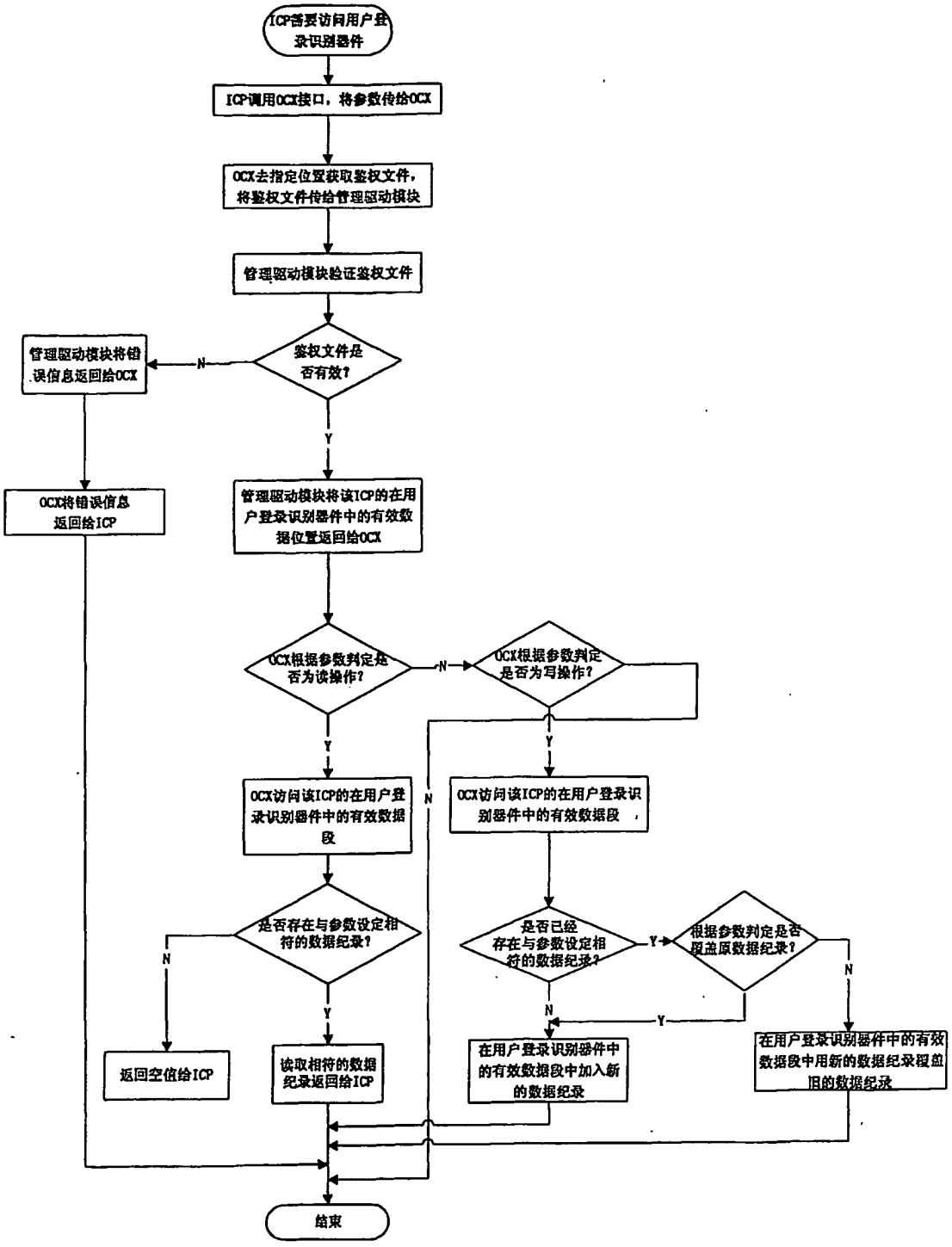
ICP需要访问用户登录识别器件
ICP调用OCX接口，将参数传给OCX
OCX去指定位置获取鉴权文件，将鉴权文件传给管理驱动模块
管理驱动模块验证鉴权文件
鉴权文件是否有效？
N
管理驱动模块将错误信息返回给OCX
OCX将错误信息返回给ICP
Y
管理驱动模块将该ICP的在用户登录识别器件中的有效数据位置返回给OCX
OCX根据参数判定是否为读操作？
N
OCX根据参数判定是否为写操作？
Y
OCX访问该ICP的在用户登录识别器件中的有效数据段
OCX访问该ICP的在用户登录识别器件中的有效数据段
是否存在与参数设定相符的数据纪录？
是否已经存在与参数设定相符的数据纪录？
Y
根据参数判定是否覆盖原数据纪录？
N
返回空值给ICP
读取相符的数据纪录返回给ICP
在用户登录识别器件中的有效数据段中加入新的数据纪录
在用户登录识别器件中的有效数据段中用新的数据纪录覆盖旧的数据纪录
结束

图 3

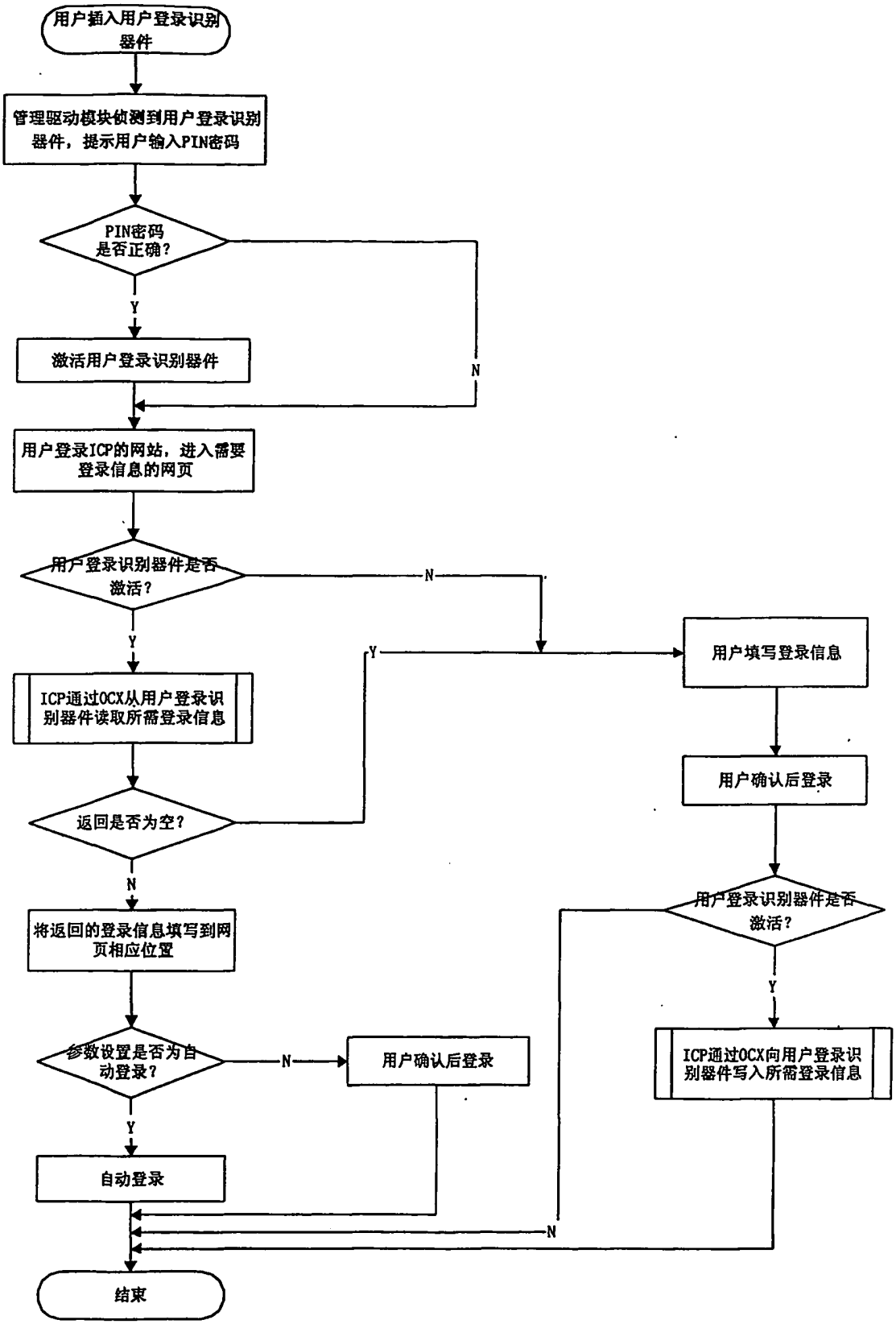
用户插入用户登录识别器件
管理驱动模块侦测到用户登录识别器件，提示用户输入PIN密码
PIN密码是否正确？
Y
N
激活用户登录识别器件
用户登录ICP的网站，进入需要登录信息的网页
用户登录识别器件是否激活？
N
Y
ICP通过OCX从用户登录识别器件读取所需登录信息
Y
用户填写登录信息
返回是否为空？
N
用户确认后登录
将返回的登录信息填写到网页相应位置
用户登录识别器件是否激活？
参数设置是否为自动登录？
N
用户确认后登录
Y
ICP通过OCX向用户登录识别器件写入所需登录信息
Y
自动登录
N
结束

图 4